Lag

om ändring av lagen om informationshantering inom den offentliga förvaltningen

I enlighet med riksdagens beslut

ändras i lagen om informationshantering inom den offentliga förvaltningen (906/2019) 2 § 16 punkten, 3 § och 10 § 1 mom. 2 punkten, av dem 2 § 16 punkten sådan den lyder i lag 488/2023 och 3 § sådan den lyder delvis ändrad i lagarna 653/2021 och 488/2023, samt

fogas till 1 § ett nytt 2 mom., i stället för det 2 mom. som upphävts genom lag 710/2021, och till 2 §, sådan den lyder delvis ändrad i lag 488/2023, nya 17—25 punkter samt till lagen ett nytt 4 a kap. som följer:

1 §

Lagens syfte

— —

Genom denna lag genomförs bestämmelserna om skyldigheter för aktörer, om tillsynen över fullgörandet av dem och om påföljder i Europaparlamentets och rådets direktiv (EU) 2022/2555 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972 och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet) inom sektorn för offentlig förvaltning som avses i punkt 10 i bilaga I till NIS 2-direktivet (*den offentliga förvaltningen*). Bestämmelser om genomförande av NIS 2-direktivet till övriga delar finns i cybersäkerhetslagen (/).

2 §

Definitioner

I denna lag avses med

— —

16) *behandlingsregler* av en fysisk person på förhand utarbetade regler avsedda att styra automatisk databehandling,

17) *kommunikationsnät och informationssystem*

a) ett elektroniskt kommunikationsnät som avses i artikel 2.1 i Europaparlamentets och rådets direktiv (EU) 2018/1972 om inrättande av en europeisk kodex för elektronisk kommunikation,

b) en enhet eller en grupp enheter som är sammankopplade eller hör samman med varandra, av vilka en eller flera genom ett program utför automatisk behandling av digitala uppgifter, och

c) digitala uppgifter som lagras, behandlas, hämtas eller överförs i sådana system som avses i underpunkt a och b för att dessa system ska kunna drivas, användas, skyddas eller underhållas,

18) *säkerhet i kommunikationsnät och informationssystem* kommunikationsnäts och informationssystems förmåga att med en viss tillförlitlighetsnivå motstå händelser som kan äventyra tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via dessa nät och system,

RP 57/2024 rd
KoUB 1/2025 rd
RSv 15/2025 rd

19) *cybersäkerhet* åtgärder som behövs för att skydda kommunikationsnät och informationssystem, deras användare och andra berörda personer mot cyberhot,

20) *cyberhot* en omständighet, händelse eller handling som när den förverkligas kan skada, störa eller på annat negativt sätt påverka kommunikationsnät och informationssystem, användare av dessa system och andra personer,

21) *betydande cyberhot* ett cyberhot som, på grund av dess tekniska egenskaper, kan antas ha potential att ha en allvarlig påverkan på en myndighets nätverks- och informationssystem eller användarna av dess tjänster genom att orsaka betydande materiell eller immateriell skada,

22) *cyberrisk* risk för förlust eller störning orsakad av en incident, som ska uttryckas som en kombination av omfattningen av förlusten eller störningen och sannolikheten för att en incident inträffar,

23) *incident* en händelse som undergräver tillgängligheten, autenticiteten, riktigheten eller konfidentialiteten hos lagrade, överförda eller behandlade uppgifter eller hos de tjänster som erbjuds genom eller är tillgängliga via kommunikationsnät och informationssystem,

24) *betydande incident* en incident som

a) har orsakat eller kan orsaka allvarliga driftsstörningar för tjänsterna eller betydande ekonomiska förluster för en myndighet, eller

b) har påverkat eller kan påverka fysiska eller juridiska personer genom att orsaka betydande materiell eller immateriell skada,

25) *incidenthantering* åtgärder och förfaranden som syftar till att förebygga, upptäcka, analysera, begränsa eller reagera på och återhämta sig från en incident.

3 §

Lagens tillämpningsområde och avgränsningar av det

Denna lag ska tillämpas på informationshantering och på användning av informationssystem, då myndigheter behandlar informationsmaterial, om inte något annat föreskrivs någon annanstans i lag. Bestämmelserna i 6 a kap. i denna lag ska tillämpas på införande och användning av *automatiserat beslutsförfarande*. Vad som i denna lag föreskrivs om myndigheter ska också tillämpas på universitet som avses i universitetslagen (558/2009) och på yrkeshögskolor som avses i yrkeshögskolelagen (932/2014).

Det föreskrivs särskilt om förfaranden som ska iakttas vid ärendehantering och tjänsteproduktion, om sekretessbeläggning och om rätten till information om myndighetshandlingar samt om arkivering av handlingar. I kyrkolagen (652/2023) föreskrivs om informationshantering och användning av informationssystem inom Finlands evangelisk-lutherska kyrka.

Bestämmelserna i 4 a kap. tillämpas inte på följande myndigheter och myndighetsverksamheter:

1) republikens presidents kansli, riksdagens ämbetsverk, Försvarsmakten, polisenheter som avses i polisförvaltningslagen (110/1992), Gränsbevakningsväsendet, Åklagarmyndigheten och Tullens brottsbekämpning,

2) domstolar och nämnder som har inrättats för att behandla besvärsärenden,

3) Försvarsfastigheter,

4) kommunala myndigheter med undantag för Helsingfors stad på vilken 4 a kap. tillämpas när staden sköter uppgifter som enligt lag hör till välfärdsområdenas organiseringsansvar,

5) Finlands Bank,

6) universitet som avses i universitetslagen, yrkeshögskolor som avses i yrkeshögskolelagen, Räddningsinstitutet och övriga statliga utbildningsinstitutioner,

7) sådan tjänsteproduktion i säkerhetsnätet och användning av dess tjänster som avses i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät (10/2015),

8) myndigheter som har inrättats tillsammans med ett land som inte hör till Europeiska ekonomiska samarbetsområdet i enlighet med en internationell överenskommelse och diplomatiska eller konsulära beskickningar i dessa länder och deras nätverks- och informationssystem, till den del dessa system finns i beskickningens lokaler eller upprätthålls för användare i ett av dessa länder.

Bestämmelserna i 19, 20, 26 och 27 § ska inte tillämpas på rättskipningen vid domstolar eller nämnder som har inrättats för att behandla besvärsärenden. Bestämmelserna i 3 kap. ska inte tillämpas på riksdagens justitieombudsmans, justitiekanslerns i statsrådet eller domstolarnas verksamhet eller verksamheten vid nämnder som har inrättats för att behandla besvärsärenden och inte heller på republikens presidents kansli, riksdagens ämbetsverk, Folkpensionsanstalten, Finlands Bank, övriga självständiga offentligrättsliga inrättningar, universitet som avses i universitetslagen eller på yrkeshögskolor som avses i yrkeshögskolelagen. Bestämmelserna i 3 kap. ska tillämpas på välfärdsområden, välfärdssammanslutningar, kommuner och samkommuner då de sköter lagstadgade uppgifter. Bestämmelserna i 18 g § 3 mom. och 18 h—18 l § ska inte tillämpas på riksdagens justitieombudsmans eller justitiekanslerns i statsrådet verksamhet.

Vad som i 4 kap., 22—24 och 25—27 § samt 6 a kap. föreskrivs om informationshanteringsenheter och myndigheter ska tillämpas på privatpersoner och privaträttsliga sammanslutningar samt sådana offentligrättsliga samfund som inte är myndigheter till den del dessa sköter offentliga förvaltningsuppgifter. På privatpersoner, privaträttsliga sammanslutningar och sådana offentligrättsliga samfund som inte är myndigheter tillämpas dessutom vad som i 4 och 28 § föreskrivs om informationshanteringsenheter när de utövar offentlig makt på det sätt som avses i 4 § 2 mom. i lagen om offentlighet i myndigheternas verksamhet eller när det särskilt föreskrivs att den lagen ska tillämpas på deras verksamhet. Vidare tillämpas vad som i 19 § 2 mom. samt i 24 a och 24 b § föreskrivs om myndigheter på privaträttsliga sammanslutningar och sådana offentligrättsliga samfund som inte är myndigheter när de utövar offentlig makt på det sätt som avses i 4 § 2 mom. i lagen om offentlighet i myndigheternas verksamhet.

Denna lag ska inte tillämpas på statliga myndigheter i landskapet Åland. Lagens 13 a § och 6 a kap. ska dock tillämpas på statliga myndigheter på Åland när de sköter sådana myndighetsuppgifter som hör till rikets lagstiftningsbehörighet och som innebär automatiserat avgörande av ärenden enligt 53 e § i förvaltningslagen. Även 4 a kap. ska tillämpas på statliga myndigheter i landskapet Åland, om inte något annat följer av 3 mom.

10 §

Den offentliga förvaltningens informationshanteringsnämnd

I anslutning till finansministeriet finns en informationshanteringsnämnd för den offentliga förvaltningen (*informationshanteringsnämnden*) med uppgift att

— —

2) främja förfarandena i fråga om informationshantering och informationssäkerhet samt genomförandet av de krav som föreskrivs i denna lag, med undantag för vad som föreskrivs i 4 a kap.

— —

4 a kap.

Skyldigheter som gäller cybersäkerhet och tillsynen över att de fullgörs

18 a §

Aktörsindelning och anmälan om verksamhet

De informationshanteringsenheter som omfattas av tillämpningsområdet för detta kapitel är väsentliga aktörer inom den offentliga förvaltningen. Välfärdsområdena och välfärdssammanslutningarna samt Helsingfors stad är dock viktiga aktörer.

En informationshanteringsenhet ska till tillsynsmyndigheten anmäla

1) sitt namn,

2) sin adress, sin e-postadress, sitt telefonnummer och sina andra aktuella kontaktuppgifter,

3) sina IP-adressintervall,

4) uppgift om huruvida den är en väsentlig eller en viktig aktör inom den offentliga förvaltningen,

5) en förteckning över övriga medlemsstater i Europeiska unionen där enheten tillhandahåller sina tjänster,

6) sitt deltagande i frivilliga arrangemang för informationsutbyte om cybersäkerhet enligt 23 § i cybersäkerhetslagen.

Informationshanteringsenheten ska utan dröjsmål, senast inom två veckor från en ändring, anmäla alla ändringar i de uppgifter som avses i 2 mom.

18 b §

Skyldighet att hantera cybersäkerhetsrisker och handlingsmodell för hantering av cybersäkerhetsrisker

En informationshanteringsenhet ska identifiera, utvärdera och hantera cyberrisker som hänför sig till säkerheten i de kommunikationsnät och informationssystem som den använder i sina funktioner eller för att tillhandahålla sina tjänster. Hanteringen av cybersäkerhetsrisker ska förhindra eller minimera incidenters inverkan på verksamheten, driftskontinuiteten, tjänstemottagarna och andra tjänster. Informationshanteringsenheten ska vidta de åtgärder för hantering av cybersäkerhetsrisker som avses i 18 c §.

Informationshanteringsenheten ska ha en uppdaterad handlingsmodell för hantering av cybersäkerhetsrisker för att skydda kommunikationsnät och informationssystem och deras fysiska miljö mot incidenter och deras verkningar. I handlingsmodellen för hantering av cybersäkerhetsrisker ska de risker som hänför sig till kommunikationsnät och informationssystem och deras fysiska miljö identifieras med beaktande av ett tillvägagångssätt som beaktar alla riskfaktorer. I handlingsmodellen ska målen, förfarandena och ansvaren för hanteringen av cybersäkerhetsrisker samt de åtgärder enligt 18 c § genom vilka kommunikationsnät och informationssystem och deras fysiska miljö skyddas mot cyberhot och incidenter fastställas och beskrivas.

Informationshanteringsenhetens ledning svarar för genomförandet av och tillsynen över hanteringen av cybersäkerhetsrisker samt godkänner handlingsmodellen för hantering av risker och utövar tillsyn över genomförandet av den. Informationshanteringsenhetens ledning ska ha tillräcklig förtrogenhet med hantering av cybersäkerhetsrisker.

18 c §

Åtgärder för hantering av cybersäkerhetsrisker

En informationshanteringsenhet ska vidta proportionella tekniska, driftsrelaterade och organisatoriska åtgärder för hantering av cybersäkerhetsrisker för att hantera sådana cyberrisker hänför sig till säkerheten i de kommunikationsnät och informationssystem som enheten använder och för att förhindra eller minimera skadliga verkningar. I handlingsmodellen för

hantering av cybersäkerhetsrisker och de åtgärder för hantering av cybersäkerhetsrisker som baserar sig på den ska åtminstone följande beaktas och hållas uppdaterat:

1) riktlinjerna för hantering av cybersäkerhetsrisker samt bedömningen av effektiviteten i fråga om åtgärderna för hantering av cybersäkerhetsrisker,

2) de riktlinjer som gäller säkerheten i kommunikationsnät och informationssystem,

3) säkerheten vid förvärv, utveckling och underhåll av kommunikationsnät och informationssystem samt behövliga förfaranden för hantering av sårbarheter och delgivning av information om sårbarheter,

4) den övergripande kvaliteten och resiliensen i leveranskedjan i fråga om direkta leverantörers produkter och tjänsteleverantörers tjänster, de åtgärder för hantering av cybersäkerhetsrisker som är inbyggda i dem och cybersäkerhetspraxis hos direkta leverantörer och tjänsteleverantörer samt resultatet av de samordnade riskbedömningar av kritiska leveranskedjor som avses i artikel 22.1 i NIS 2-direktivet,

5) tillgångsförvaltningen och identifieringen av funktioner som är viktiga med tanke på dess säkerhet,

6) personalsäkerheten och utbildningen i cybersäkerhet,

7) förfarandena för åtkomsthantering och autentisering,

8) riktlinjerna och förfarandena för användning av krypteringsmetoder samt vid behov åtgärderna för användning av säker elektronisk kommunikation,

9) upptäckandet och hanteringen av incidenter i syfte att upprätthålla och återställa säkerheten och driftssäkerheten,

10) säkerhetskopieringen, katastrofhanteringen, krishanteringen och den övriga driftskontinuiteten samt vid behov användningen av säkrade reservkommunikationssystem,

11) grundläggande praxis för informationssäkerhet för att säkerställa verksamheten samt säkerheten i datakommunikationen, maskinvaran, programvaran och datamaterialet,

12) åtgärderna för att skydda den fysiska miljön i fråga om kommunikationsnät och informationssystem samt säkerställa lokalsäkerheten och nödvändiga resurser.

Åtgärderna ska vara aktuella, lämpliga och proportionella i förhållande till riskexponeringen när det gäller de kommunikationsnät och informationssystem som informationshanteringsenheten använder, kommunikationsnätets eller informationssystemets betydelse för informationshanteringsenhetens verksamhet samt de direkta konsekvenser som en incident i dessa rimligtvis kan förutses ha. Vid dimensioneringen av åtgärderna ska informationshanteringsenhetens storlek, arten av dess verksamhet, sannolikheten för att incidenter inträffar och deras allvarlighetsgrad, kostnaderna för åtgärderna samt de tekniska medel för att avvärja cyberhot som med beaktande av den aktuella utvecklingen är tillgängliga dessutom beaktas.

I riskhanteringen, i handlingsmodellen för hantering av risker och vid genomförandet av riskhanteringsåtgärder ska dessutom Europeiska kommissionens genomförandeakter som eventuellt antas med stöd av artikel 21.5 i NIS 2-direktivet iakttas.

18 d §

Skyldighet att anmäla betydande incidenter

Myndigheten ska utan dröjsmål, senast inom 24 timmar från upptäckten av en betydande incident lämna tillsynsmyndigheten en första anmälan om incidenten, i vilken det ska anges om incidenten misstänks ha orsakats av ett brott eller av andra olagliga eller avsiktligt skadliga handlingar och om incidenten kan ha gränsöverskridande verkningar samt sannolikheten för sådana verkningar.

Myndigheten ska utan dröjsmål, senast inom 72 timmar från upptäckten av en betydande incident lämna tillsynsmyndigheten en uppföljande anmälan om incidenten, i vilken den information som avses i 1 mom. ska uppdateras och det ska anges en inledande bedömning av

den betydande incidentens art, allvarlighetsgrad och konsekvenser samt, i förekommande fall, angreppsindikatorer.

Myndigheten ska inom en månad från det att den uppföljande anmälan lämnades in lämna tillsynsmyndigheten en slutrapport om den betydande incidenten. Slutrapporten ska innehålla

1) en detaljerad beskrivning av incidenten, dess allvarlighetsgrad och konsekvenser,

2) en redogörelse för den typ av hot eller grundorsak som sannolikt har utlöst incidenten,

3) en redogörelse för tillämpade och pågående åtgärder för att begränsa konsekvenserna av incidenten, och

4) en redogörelse för eventuella gränsöverskridande konsekvenser.

Om incidenten fortfarande fortgår när den slutrapport som avses i 3 mom. ska lämnas in, ska en delrapport om hur hanteringen av incidenten framskrider lämnas i stället för slutrapporten. Slutrapporten ska då lämnas in inom en månad från det att myndigheten har hanterat incidenten. När incidenten fortgår har tillsynsmyndigheten rätt att av myndigheten få ytterligare information eller en delrapport.

Vid anmälan av en betydande incident ska dessutom iakttas Europeiska kommissionens genomförandeakter som eventuellt antas med stöd av artikel 23.11 i NIS 2-direktivet och som gäller typen av information i och formatet och förfarandet för anmälan samt en närmare definition av betydande incidenter.

18 e §

Mottagande av incidentanmälan

Tillsynsmyndigheten ska utan dröjsmål, om möjligt inom 24 timmar från mottagandet av den första anmälan som avses i 18 d § 1 mom., lämna ett svar till myndigheten. Svaret ska innehålla initial återkoppling om den betydande incidenten och, på myndighetens begäran, vägledning eller operativa råd om hanteringen av incidenten samt vägledning om hur den betydande incidenten ska anmälas till förundersökningsmyndigheten, om brott misstänks i ärendet.

Tillsynsmyndigheten ska när den ger vägledning och operativa råd som avses i 1 mom. samarbeta med den CSIRT-enhet som avses i cybersäkerhetslagen. Vägledning och operativa råd kan ges av CSIRT-enheten i stället för av tillsynsmyndigheten.

18 f §

Frivillig underrättelse

En myndighet kan underrätta tillsynsmyndigheten också om andra än betydande incidenter samt om cyberhot och tillbud. Även de som avses i 3 §, på vilka detta kapitel inte tillämpas, kan göra en sådan underrättelse.

Tillsynsmyndigheten ska behandla frivilliga underrättelser som avses i 1 mom. med iakttagande av det förfarande som anges i 18 e §. Tillsynsmyndigheten får prioritera behandlingen av anmälningar som avses i 18 d § i förhållande till behandlingen av frivilliga underrättelser.

Myndigheter och andra som avses i 3 § kan i samband med en frivillig underrättelse lämna ut sådan information till tillsynsmyndigheten som tillsynsmyndigheten har rätt att få med stöd av 18 i §.

I samband med en frivillig underrättelse ska dessutom Europeiska kommissionens genomförandeakter som eventuellt antas med stöd av artikel 23.11 i NIS 2-direktivet och som gäller typen av information i och formatet och förfarandet för underrättelser iakttas.

18 g §

Informationsskyldighet om betydande cyberhot och incidenter

En myndighet ska utan dröjsmål underrätta mottagarna av sina tjänster om en betydande incident, om den betydande incidenten sannolikt inverkar negativt på tillhandahållandet av dess tjänster.

En myndighet ska utan dröjsmål underrätta de mottagare av sina tjänster som kan påverkas av ett betydande cyberhot om ett betydande cyberhot och om de åtgärder som står till buds för att hantera cyberhotet.

Om det ligger i allmänt intresse att det informeras om en betydande incident, kan tillsynsmyndigheten ålägga myndigheten att informera om den betydande incidenten eller själv informera om saken.

I den informering som avses i 1 och 2 mom. ska dessutom Europeiska kommissionens genomförandeakter som eventuellt antas med stöd av artikel 23.11 i NIS 2-direktivet och som gäller typen av information i och formatet och förfarandet för underrättelser samt en närmare definition av betydande incidenter iakttas.

18 h §

Tillsynsmyndighet

Transport- och kommunikationsverket är den tillsynsmyndighet som avses i detta kapitel och den behöriga myndigheten inom den offentliga förvaltningen som avses i artikel 8.1 i NIS 2-direktivet. Utöver vad som föreskrivs i detta kapitel ska tillsynsmyndigheten utöva tillsyn över att de skyldigheter som föreskrivs i detta kapitel och i bestämmelser som antagits med stöd av NIS 2-direktivet fullgörs inom den offentliga förvaltningen samt föra en förteckning över aktörerna inom den offentliga förvaltningen med de uppgifter som lämnats med stöd av 18 a §. Transport- och kommunikationsverket är självständigt och oberoende i sin verksamhet som tillsynsmyndighet.

Tillsynsmyndigheten kan ställa de tillsynsuppgifter som anges i denna lag i prioritetsordning enligt en riskbaserad bedömning. Tillsynsmyndigheten ska när den inriktar tillsynen och fattar ett tillsynsbeslut enligt 18 l § beakta de omständigheter som avses i 27 § 3 mom. och 37 § i cybersäkerhetslagen. Tillsynsmyndigheten kan inrikta tillsynen gentemot ett välfärdsområde, en välfärdssammanslutning eller Helsingfors stad endast om det finns en grundad anledning att misstänka att området, sammanslutningen eller staden inte har iakttagit bestämmelserna i detta kapitel eller i rättsakter som antagits med stöd av NIS 2-direktivet.

Om inte något annat föreskrivs i detta kapitel ska tillsynsmyndigheten vid behandlingen av sådana anmälningar om verksamhet som avses i 18 a §, av sådana anmälningar och underrättelser om incidenter som avses i 18 d och 18 f § och av annan information som erhållits i samband med tillsynsuppgiften samt i samarbetet med andra myndigheter och Europeiska unionens institutioner, decentraliserade byråer och samarbetsorgan samt vid utlämnandet av information till dem iaktta vad som i 6 § 4 mom., 15 § 3 mom., 17 §, 18 § 3 mom., 26 § 2 mom., 28 § 4 och 5 mom., 33 §, 41 § 5 mom. och 45 § i cybersäkerhetslagen föreskrivs om behandling av information vid tillsynsmyndigheten, om tillsynsmyndighetens samarbete med andra myndigheter och Europeiska unionens institutioner, decentraliserade byråer och samarbetsorgan samt om utlämnandet av information till dem.

Bestämmelser om Transport- och kommunikationsverkets uppgifter som gemensam kontaktpunkt och CSIRT-enhet enligt NIS 2-direktivet finns i cybersäkerhetslagen.

18 i §

Tillsynsmyndighetens rätt att få information

Tillsynsmyndigheten har när den utför uppgifter enligt detta kapitel trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att få information om hanteringen av cybersäkerhetsrisker, handlingsmodellen för riskhantering, hanteringsåtgärderna och betydande incidenter samt annan information som direkt anknyter till ovannämnda information och som är nödvändig för tillsynen över fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker och över anmälan och rapporteringen av betydande incidenter. Myndigheten ska lämna ut informationen utan dröjsmål och avgiftsfritt.

Tillsynsmyndigheten har trots sekretessbestämmelserna och andra begränsningar som gäller utlämnande av information rätt att av en myndighet få förmedlingsuppgifter, lokaliseringsuppgifter och information om meddelanden som innehåller ett skadligt datorprogram eller ett skadligt kommando, om det är nödvändigt för tillsynen över fullgörandet av den skyldighet som gäller hantering av cybersäkerhetsrisker eller över anmälan och rapporteringen av betydande incidenter. Den information som tillsynsmyndigheten fått med stöd av detta moment är sekretessbelagd.

Rätten till information enligt denna paragraf gäller inte sekretessbelagd information om sådan tjänsteproduktion eller användning av tjänster i säkerhetsnätet som avses i lagen om verksamheten i den offentliga förvaltningens säkerhetsnät eller information vars utlämnande skulle äventyra försvaret eller den nationella säkerheten eller strida mot ett viktigt intresse i samband därmed.

Bestämmelser om de förpliktelser som gäller hantering av särskilt känsligt informationsmaterial finns i lagen om internationella förpliktelser som gäller informationssäkerhet.

18 j §

Tillsynsmyndighetens rätt att förrätta inspektioner

Tillsynsmyndigheten har rätt att i den omfattning som det behövs förrätta inspektion av en myndighet för tillsynen över att de skyldigheter som föreskrivs i detta kapitel eller i bestämmelser som antagits med stöd av NIS 2-direktivet fullgörs.

Den som förrättar inspektionen ska ha tillräcklig utbildning och erfarenhet med hänsyn till inspektionens art och omfattning.

Myndigheten ska i den omfattning som inspektionen förutsätter ge den som förrättar inspektion tillträde till det kommunikationsnät eller informationssystem som inspektionen gäller och till andra utrymmen än sådana som är avsedda för boende av permanent natur. För förrättande av inspektionen har den som förrättar inspektionen trots sekretessbestämmelserna eller andra begränsningar som gäller utlämnande av information rätt att få granska den information och de handlingar, maskinvaror och programvaror som är nödvändiga för tillsynsuppgiften, utföra behövliga tester och mätningar samt granska de säkerhetsarrangemang som myndigheten har genomfört. På inspektionsförrättarens rätt att förrätta inspektion och få information tillämpas vad som i 18 i § 3 mom. föreskrivs om begränsningar i rätten att få information.

På förfarandet vid inspektionen tillämpas vad som i 39 § i förvaltningslagen föreskrivs om inspektion.

18 k §

Tilldelande av biträdande uppgift till bedömningsorgan för informationssäkerhet samt att låta utföra bedömning

Tillsynsmyndigheten kan tilldela ett godkänt bedömningsorgan för informationssäkerhet som avses i lagen om bedömningsorgan för informationssäkerhet (1405/2011) en biträdande uppgift i anslutning till ett inspektionsuppdrag enligt 18 j §.

Tillsynsmyndigheten kan för tillsynen ålägga en myndighet att låta ett bedömningsorgan för informationssäkerhet utföra en bedömning av hanteringen av cybersäkerhetsrisker, om

1) myndigheten har drabbats av en betydande incident som har orsakat en allvarlig driftsstörning för tjänsterna eller orsakat betydande materiell eller immateriell skada, eller

2) myndigheten väsentligt och allvarligt har försummat att iaktta skyldigheterna att hantera cybersäkerhetsrisker enligt 18 b eller 18 c §.

På den som är anställd vid ett bedömningsorgan för informationssäkerhet och som bistår vid en inspektion och på en person som utför en bedömning tillämpas vad som i 18 j § 2—4 mom. föreskrivs om inspektionsförrättares erfarenhet och utbildning samt inspektionsförrättares rättigheter. Om inte något annat föreskrivs i detta kapitel, tillämpas lagen om bedömningsorgan för informationssäkerhet på bedömningsorganet för informationssäkerhet. På den som är anställd vid ett bedömningsorgan för informationssäkerhet tillämpas bestämmelserna om straffrättsligt tjänsteansvar för tjänstemän, med undantag för bestämmelserna om avsättningspåföljd, när han eller hon sköter uppgifter som avses i denna paragraf. Bestämmelser om skadeståndsansvar finns i skadeståndslagen.

18 l §

Påföljder

Tillsynsmyndigheten kan ålägga en myndighet att inom utsatt tid avhjälpa bristerna i fullgörandet av skyldigheterna enligt detta kapitel eller bestämmelser som antagits med stöd av NIS 2-direktivet. Tillsynsmyndigheten kan ålägga myndigheten att offentliggöra dessa brister eller andra omständigheter som har samband med överträdelser av de nämnda skyldigheterna.

Tillsynsmyndigheten kan ge myndigheten en varning, om den inte har fullgjort de skyldigheter som föreskrivs i detta kapitel eller i bestämmelser som antagits med stöd av NIS 2-direktivet. I varningen ska den brist eller försummelse som varningen gäller specificeras. Varningen ska ges skriftligen.

Tillsynsmyndigheten kan förena ett beslut som avses i 1 mom. med vite.

18 m §

Sökande av ändring

Bestämmelser om sökande av ändring i förvaltningsdomstol finns i lagen om rättegång i förvaltningsärenden (808/2019).

Bestämmelser om sökande av ändring i beslut som gäller föreläggande och utdömande av vite finns i viteslagen (1113/1990).

———

Denna lag träder i kraft den 8 april 2025.

Den anmälan som avses i 18 a § 2 mom. ska göras senast inom en månad från det att denna lag trätt i kraft.

Helsingfors den 4 april 2025

Republikens President

Alexander Stubb

Kommunikationsminister Lulu Ranne